



Qualys WAS Lab Tutorial Supplement

TABLE OF CONTENTS

WAS KNOWLEDGEBASE	3
WAS WORKFLOW	5
BASIC APPLICATION SETUP	6
SCHEDULED SCANS	14
WAS SITEMAP	15
OPTION PROFILE	16
QUALYS BROWSER RECORDER CRAWL SCRIPT	20
WAS REPORTING	22
TAGGING	23
USER MANAGEMENT	25
BURP INTEGRATION	27
QUALYS WAS CERTIFICATION EXAM	28

Qualys Web Application Scanning (WAS) enables organizations to assess, track, and remediate Web application vulnerabilities. With BURP integration, manual Web application testing results can be combined with the automated findings produced by WAS. The Qualys Malware Detection (MD), is a standard component in WAS, providing malware monitoring on top of vulnerability detection.

The Open Web Application Security Project (OWASP) Top 10 list has become the industry standard for categorizing the most critical risks faced by Web apps. Qualys WAS allows you to accurately find these vulnerabilities – including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and URL redirection – and learn how to mitigate them.

WAS KnowledgeBase



All detectable vulnerabilities can be viewed from the Qualys KnowledgeBase. The Search and Filtering pane (left) will allow you to locate Web application vulnerabilities.

QID	Name	Information	Category	Severity
150300	HTTP Request Smuggling	+	Web Application	High
150261	Subresource Integrity (SRI) Not Implemented	+	Web Application	Medium
150326	Atlassian Jira Server and Data Center Information Disclosure vulnerability	+	Web Application	High
150324	Atlassian Jira Server and Data Center Information Disclosure vulnerability	+	Web Application	High
150325	Adobe Experience Manager CMS Detected	+	Web Application	Medium
150303	SAP NetWeaver Application Server JAVA (LM Configuration Wizard) Multiple Vulnerabilities	+	Web Application	High
150312	vBulletin Pre-authentication remote command execution vulnerability (CVE-2019-16759)	+	Web Application	High
150323	WordPress Email Subscribers and Newsletters plugin unauthenticated email forgery/spoofing Vulnerability	+	Web Application	High

WAS Search Lists



A “Search List” is an extension of the Qualys KnowledgeBase and is a powerful customization tool within Qualys Web Application Scanning. The name “Search List” is derived from the KnowledgeBase “Search” tool that is used to create a list of vulnerabilities. A Search List is a grouping of QIDs that can be used in various capacities in Qualys Web Application Scanning.

You can add a Search List to an Option Profile to customize your scan. For instance, you can run a scan for just a specific vulnerability. Or, you can use a Search List to omit vulnerabilities from a scan.

You can also add a Search List to a Report Template to help prioritize which vulnerabilities will be addressed first. For example, you can build a report containing only XSS vulnerabilities or only your most severe vulnerabilities.

Option Profiles Bruteforce Lists Search Lists Parameter Sets DNS Override Appliances Global Settings			
Actions (0) New List		1 - 3 of 3	
<input type="checkbox"/> Name	Type	Owner	
<input type="checkbox"/> XSS Vulns	Static	Training User (quays3tr17)	
<input type="checkbox"/> Worst Vulnerabilities	Dynamic	Training User (quays3tr17)	
<input type="checkbox"/> Authentication Test	Static	System	

WAS Workflow

The workflow for analyzing a Web application involves five simple steps: 1) Define Web Application, 2) Perform Discovery Scan—Crawl, 3) Perform Vulnerability Scan, 4) Create Reports, and 5) Fix Vulnerabilities

Here is a detailed view of this workflow:

1. Define Web Application
 - Identify the location (URL) of the Web App
 - Define the “scope” of the Web App Crawl
 - Choose from various scanning options—Option Profile:
 - Select a scanner appliance
 - Include “crawling hints” and/or header injection
 - Use optional DNS Override
 - Provide authentication credentials
 - Form records
 - Server records
 - Identify areas to “white list” or “black list”
 - Enable malware monitoring
2. Perform Discovery Scan (Crawl)
3. Perform Vulnerability Scan
4. Create reports to identify links crawled and vulnerabilities detected
5. Fix vulnerabilities

Basic Application Setup

PLAY → <http://ior.ad/7eMQ>

PLAY → <http://ior.ad/7eVu>

Before a Web Application can be scanned, it must first be added to your WAS subscription.

The screenshot shows the 'Web Application Creation' wizard, Step 1 of 11: Asset Details. The left sidebar lists 11 steps: 1. Asset Details (selected), 2. Application Details, 3. Scan Settings, 4. Crawl Settings, 5. Redundant Links, 6. Authentication, 7. Exclusions, 8. Advanced Options, 9. Malware Monitoring, 10. Comments, and 11. Review And Confirm. The main content area is titled 'Tell us about the asset you want to scan' and contains the following sections:

- Definition** (marked as a required field): A text input field for the asset name, with 'Demo' entered.
- Target Definition**: A text input field for the Web Application URL (or Swagger file URL), with 'http:// 54.173.177.208:8080/bodgeit/home' entered. A note below states: 'For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications or APIs that you specify as scan targets.'
- Custom Attributes**: A table for providing attribute information to categorize the web application within the subscription.

Name	Value
Business Function	Online Store

An 'Add' button is located to the right of the table. Below the table is a 'Tags' section with the text 'Select tags to apply to the web application' and links for 'Select', 'Create', and 'Remove All'. At the bottom of the wizard are 'Cancel' and 'Continue' buttons.

On Step 1 (Asset Details) of defining the web application, the following can be defined:

Target definition – URL of the application or the Swagger file if you’re scanning API endpoints

Custom Attributes – Name/Value pairs that can be used for categorizing and filtering the application

Tags – Labels that can be applied to applications for filtering, scanning, and reporting purposes

Web Application Creation
Turn help tips: On | Off Launch help

Step 2 of 11

1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Malware Monitoring
10 Comments
11 Review And Confirm

Tell us about the web application you want to scan

Target Definition
(*) REQUIRED FIELDS

Web Application URL (or Swagger file URL)
http://54.173.177.208:8080/bodgeit/home.jsp

Crawl Scope*

Limit at or below URL hostname (54.173.177.208)

Scope will be limited to the hostname within the URL: http://54.173.177.208:8080/bodgeit/, using HTTP or HTTPS and any port. All links discovered on the 54.173.177.208 domain will be in scope. For example, all links discovered in http://54.173.177.208:8080/support/ and https://54.173.177.208:8080/logout/ will be in scope. Links outside the 54.173.177.208 domain are not in scope.

Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location

API Endpoint Definition (non-Swagger based APIs)

☒ None
☐ Postman Collection

Upload a valid Postman Collection file for your API. We currently only support v2.0.0 and v2.1.0. for Postman

On Step 2 (Application Details) of defining the web application, the following can be defined:

Crawl Scope – a single web application can span multiple domains, IP addresses, and port numbers (including sub-domains and subdirectories). The scope of an application defines its boundaries.

The “Crawl Scope” field provides a few options:

- **Limit at or below URL hostname** - Select to limit crawling to the hostname within the URL, using HTTP or HTTPS and any port.
- **Limit to content located at or below URL subdirectory** - Select to crawl all links starting with a URL subdirectory using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified sub-domain** - Select this option to crawl only the URL hostname and one specified sub-domain, using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified domains** - Select this option to crawl only the URL hostname and specified domains, using http or https and any port.

Explicit URLs to Crawl - this is useful for pages not directly linked to other pages within the application. For example, a registration link sent to the user via email. You can also include WSDL URLs for web services you want the service to crawl. Enter each URL on a separate line.

Each entry must be a valid http or https URL. You can enter a maximum of 2048 characters for each URL. The URLs you enter must be consistent with the selected scope.

API Endpoint Definition – for non-Swagger based APIs, you may upload a valid Postman collection or a Burp Log file with your scan tests

Web Application Creation Turn help tips: On | Off Launch help X

Step 3 of 11

- 1 Asset Details ✓
- 2 Application Details ✓
- 3 Scan Settings** ✓
- 4 Crawl Settings ✓
- 5 Redundant Links ✓
- 6 Authentication
- 7 Exclusions
- 8 Advanced Options
- 9 Malware Monitoring
- 10 Comments
- 11 Review And Confirm

Tell us the scan settings you'd like to use

Default Scan Options (*) REQUIRED FIELDS

Choose the default scan settings for your web application. You can change the defaults for each scan.

Option Profile
None View Create

Scanner Appliance

Choose the default scanner appliance for your web application. You can change the defaults for each scan

☒ External ☐ Individual ☐ Tags (Scanner pool)

☐ Lock this scanner appliance for this web application.

Duration

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.
When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.

Cancel Option
Do not Cancel Scan

Cancel Previous Continue

On Step 3 (Scan Settings) of defining the web application, the following can be defined:

Option Profile – A collection of scan settings to be used while crawling or scanning the application

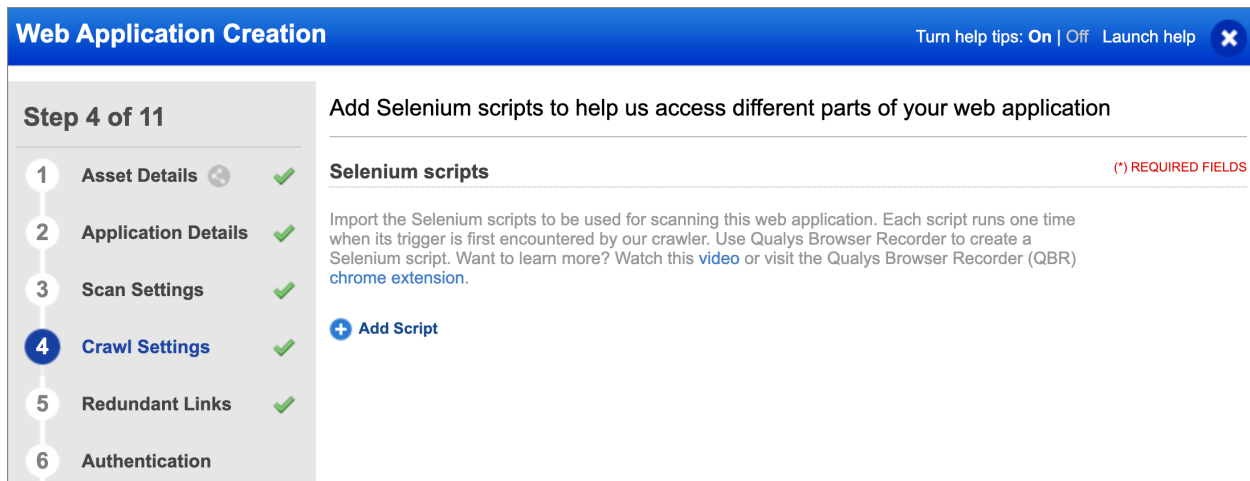
Scanner Appliance – The appliance to be used for crawling or scanning the application. Be sure the Scanner Appliance you are using has access to the application you are scanning.

Duration – How long should the scan run before being automatically cancelled

Crawling hints - Instruct the scan to adhere to existing configurations when scanning the web application using a robots.txt or sitemap.xml file

Header injection - Headers that need to be injected by our scanning service to scan the web application. This option is intended to be used when a workaround is needed for complex authentication schemes or to impersonate a web browser

Examples of header injection - https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/web_applications/scan_settings.htm



Web Application Creation Turn help tips: On | Off Launch help

Step 4 of 11

- 1 Asset Details ✓
- 2 Application Details ✓
- 3 Scan Settings ✓
- 4 Crawl Settings ✓**
- 5 Redundant Links ✓
- 6 Authentication

Add Selenium scripts to help us access different parts of your web application

Selenium scripts (*) REQUIRED FIELDS

Import the Selenium scripts to be used for scanning this web application. Each script runs one time when its trigger is first encountered by our crawler. Use Qualys Browser Recorder to create a Selenium script. Want to learn more? Watch this [video](#) or visit the Qualys Browser Recorder (QBR) [chrome extension](#).

+ Add Script

On Step 4 (Crawl Settings) of defining the web application, the following can be defined:

Selenium Script – Upload Selenium scripts recorded using Qualys Browser Recorder to play back functions in web applications during scanning

Web Application Creation
Turn help tips: On | Off Launch help

Step 5 of 11

1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Malware Monitoring
10 Comments
11 Review And Confirm

Specify redundant links in your web application

Redundant Links

Specify links in the web applications for which contents are the same and because of which scan may spend too much time crawling and assessing these URLs. Links shall be specified as regular expressions so that you can specify an expression to match a list of links.

Check [guide](#) on how to format your regular expressions.

Specify the number of instances to be tested for each link identified by above regular expressions.

Max. Links to Crawl*

5

Path Fuzzing Rules

Path fuzzing rules allow the scanner to interpret URL path components as application parameters when your web

Cancel

Previous

Continue

On Step 5 (Redundant Links) of defining the web application, the following can be defined:

Redundant Links – Links in the application that have the same content and may result in the scanner spending too much time crawling and assessing these URLs

Path Fuzzing Rules – If your application uses URL rewrite, use path fuzzing rules to specify the path components that need to be tested. More information can be found here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/path_fuzzing_rules.htm

Web Application Creation
Turn help tips: On | Off Launch help

Step 6 of 11

1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication

Set up authentication for your web application

Authentication Records
(*) REQUIRED FIELDS

Select one or more authentication records to be used for scanning this web application. Each record will define one or more authentication methods (Basic, Server, NTLM).

Records
Please select an Authentication Record
Create Remove all

BoQ Authentication
Set as Default View Edit Remove

On Step 6 (Authentication), you may define an authentication record to be used for authenticating into the web application.

Web Application Creation
Turn help tips: On | Off Launch help

Step 7 of 11

1 Asset Details
2 Application Details
3 Scan Settings
4 Crawl Settings
5 Redundant Links
6 Authentication
7 Exclusions
8 Advanced Options
9 Malware Monitoring
10 Comments
11 Review And Confirm

Set up Exclusion Lists

URLs

White List

Set up a white list to allow links to be scanned even if a black list would normally block it. If you define a white list and black list, then a default black list equivalent to "block all URLs" is assumed.

☐ URLs
☐ Regular Expressions

Black List

Set up a black list to prevent those URLs or their sub-directories from being scanned. Any link that matches a black list entry will not be scanned unless it also matches a white list entry.

☐ URLs
☐ Regular Expressions

POST Data Black List

Cancel
Previous Continue

On Step 7 (Exclusions) of defining the web application, the following can be defined:

White List – add URLs to white list to allow them to be scanned even if a black list would block it

Black List – Add URLs to blacklist to prevent them and their sub-directories from being scanned

POST Data Black List - Define POST data lists to ensure blocking of form submission for POST requests in your web application as this could have unwanted side effects like mass emailing

Logout Regular Expression - Define logout regular expression to ensure that the logout links of your web application will not be scanned

Parameters – Define parameters to ensure these will be excluded from testing to improve scan efficiency

Read more about exclusion lists here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/web_crawling_and_black_lists.htm

The screenshot shows the 'Web Application Creation' interface at Step 8 of 11, titled 'Advanced Options'. On the left, a vertical list of steps (1-8) is shown, with Step 8 'Advanced Options' highlighted. The main content area is divided into two sections: 'Default DNS Override' and 'Form Training'. The 'Default DNS Override' section includes a description, a list of records (currently empty with a placeholder 'Please select a DNS override record'), and a 'Create' button. The 'Form Training' section includes a description and an 'Add Form' button. The interface has a blue header bar with 'Web Application Creation' and 'Turn help tips: On | Off Launch help'.

Web Application Creation Turn help tips: On | Off Launch help

Step 8 of 11

- 1 Asset Details ✓
- 2 Application Details ✓
- 3 Scan Settings ✓
- 4 Crawl Settings ✓
- 5 Redundant Links ✓
- 6 Authentication ✓
- 7 Exclusions ✓
- 8 Advanced Options**

Advanced Options

Default DNS Override (*) REQUIRED FIELDS

Select one or more DNS override records with mappings you'd like to use by default when scanning this web application.

Records:

No DNS override records have been selected

Form Training

Provide a list of form field values to be used for submitting HTML Forms during crawling.

On Step 8 (Advanced Options) of defining the web application, the following can be defined:

DNS Override - By default the scanner uses the DNS for the web application URL to crawl the web app and perform scanning. Select a DNS override record, to use the mappings in your record

Form Training - Define an action URI, specific form field and its value to be substituted during crawling and fuzzing. This feature allows you to override a specific field's value in any given form

Web Application Creation

Turn help tips: On | Off Launch help

Step 9 of 11

1 Asset Details

2 Application Details

3 Scan Settings

4 Crawl Settings

5 Redundant Links

6 Authentication

7 Exclusions

8 Advanced Options

9 Malware Monitoring

Malware Monitoring

MD

(*) REQUIRED FIELDS

By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for all malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.

Status

☐ Enable Malware Monitoring for this web application

On Step 9 (Malware Monitoring), configure a malware scan to scan your web application for malwares. Read more here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/malware_monitoring.htm

Scheduled Scans



Any scan that can be performed manually, can also be scheduled to run automatically, on a regular basis. This way you always have the most up-to-date security information in your account.

Scan List Schedules Option Profiles Defaults					
Actions (0) New Schedule		1 - 2 of 2			
	Name	Target	Next Date	Scanned	Scan Status
<input type="checkbox"/>	Web Application Discovery Scan - 2020-10-12 Second Web App - BoQ	Second Web App - BoQ	04 Nov 2020	–	–
<input type="checkbox"/>	Scheduled scan for My First App My First App	My First App	–	06 Oct 2020	Finished

Setting up a scheduled scan is similar to setting up a regular WAS scan – provide information such as application and scanner appliance details, and then provide scheduling and notification information.

WAS Sitemap



The Web Application Sitemap gives you a convenient way to get a list of all pages/links scanned with views on the links crawled, vulnerabilities and sensitive content detected.

Web Application Sitemap: My First App

Use the filters below to alter list view for this application sitemap.

Page view filters: **C** Crawled **27** **R** Rejected **0** **E** External **0** **V** Vulnerabilities **35** **S** Sensitive Contents **0**

Link in view: » 54.173.177.208:8080 / bodgeit

Actions (0) Export Sitemap 1 - 20 of 26

Link	Link Info.	Children Info.
..		—
images		2
about.jsp	C 3	—
advanced.jsp	C	—
basket.jsp	C 4	—
contact.jsp	C 4	—
home.jsp	C 3	—
login.jsp	C 8	—
product.jsp?prodid=15	C	—
product.jsp?prodid=18	C	—
product.jsp?prodid=20	C	—
product.jsp?prodid=23	C	—
product.jsp?prodid=24	C	—
product.jsp?prodid=3	C	—
product.jsp?prodid=30	C	—

Folder Information

Folder: <http://54.173.177.208:8080/bodgeit/>
Status: **Crawled**
Vulnerabilities: **6**
Sensitive Content: **0**

Children Information

Pages Crawled: **26** Vulnerabilities: **29**

Assessment Details

Total Vulnerabilities: **29**

- 2 Level 5
- 1 Level 4
- 10 Level 3
- 2 Level 2
- 14 Level 1

Crawling Details

50

The following page view filters are available when viewing the sitemap:

Crawled – Only show pages that have been crawled during the scan

Rejected – Only show pages that have been rejected (this could be due scan permissions or configured blacklists)

External – Only show pages that contain external links (not in scope)

Vulnerabilities – Only show pages on which vulnerabilities have been detected

Sensitive content – Only show pages on which sensitive content has been detected (for example credit card numbers and social security numbers)

Option Profile



The following options are available under the **Scan Parameters** section of an Option Profile:

Option Profile Creation

Turn help tips: On | Off Launch help

Step 2 of 5

1 Profile Details

2 Scan Parameters

3 Search Criteria

4 Comments

5 Review And Confirm

Please define how the scan will perform

General Settings

(*) REQUIRED FIELDS

Form Submission*

Post & Get

Form Crawl Scope

☐ Include form action URI in form uniqueness calculation.

When enabled, we'll calculate form uniqueness using form action URI in addition to form field names. This results in crawling of all forms having same fields but having different action URI.

Maximum links to test in scope*

1000

Total number of links and forms to follow and test within the scan scope. If performing a Discovery Scan, this is the maximum links that will be crawled, as there will not be any testing performed

User Agent

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit

Request Parameter Set*

Initial Parameters (Default)

View | Create

Document Type

☒ Ignore common binary files based on file extensions.

Crawling Options

☐ Enhanced Crawling

When enabled we will attempt to load and render individual directories. If unique content is found, we'll begin crawling from there to improve scan coverage.

☒ Enable SmartScan

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

You can customize the number of actions that can be tested per page. Note the higher the number you set, the longer the scan duration.

SmartScan Depth

5

Behavior Settings

These settings define the threshold to be reached before stopping the scan. If you deactivate these settings, the scan will keep running no matter how many errors it will find.

☒ Timeout Error Threshold

100

☒ Unexpected Error Threshold

300

Performance Settings

☒ Pre-defined☐ Custom

Scan Intensity

Low

of HTTP Threads: 2

Bruteforcing Settings

☒ Use password bruteforcing

☐ User list

☒ System list

Minimal

Cancel

PreviousContinue

Form Submission - When forms are submitted, http(s) uses GET or POST methods. The crawl can be limited to either type of form submission, both, and none. It is considered best practice to select “Post & Get” for the most thorough vulnerability analysis. If “none” is chosen, the only forms WAS will submit will be for authentication

Form Crawl Scope – By default, the scanner uses form names to determine the uniqueness of a form. When “Include form action URI in form uniqueness calculation” is enabled, the scanner uses the form action URI and the form field name to determine its uniqueness

Form Crawl Scope	<input checked="" type="checkbox"/> Include form action URI in form uniqueness calculation.
------------------	---

Maximum links to test in scope – Specify the maximum links and forms to crawl during the scan. The maximum is 8000.

User Agent - If your web application requires specific user-agent string to access it, you need to specify the same. The default user agent setting that is used is user-agent: ***Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko) Version/9.0.3 Safari/601.4.4***

Request Parameter Set – Specify the default parameters that need to be injected into your web application, such as first name, last name, email address, phone number etc.

Document Type – Enable the “Ignore common binary files” option to not scan files with extensions pdf, zip, and doc.

Document Type	<input checked="" type="checkbox"/> Ignore common binary files based on file extensions .
---------------	---

Enhanced Crawling – When enabled, the scanner will attempt to load and render individual directories.

For example, if this link is found during crawling:

<https://www.example.com/foo/abc/xyz/register.php>

The scanner will make the first request to <https://www.example.com/foo/abc/xyz> and will then remove the directory “xyz” from the URL and crawl, <https://www.example.com/foo/abc/> and later it will further remove “abc/” and will crawl <https://www.example.com/foo/> .

All links found during this process of removal and re-crawling will get added to the crawl queue, thus improving the scan coverage.

Enable SmartScan – When enabled, the scanner will perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing. This option is recommended for scanning applications with advanced frameworks and technologies.

Timeout Error Threshold – Maximum number of timeout errors encountered during the scan that will result in the scan being terminated.

Unexpected Error Threshold - Maximum number of unexpected errors encountered during the scan that will result in the scan being terminated.

Performance Settings – select from Pre-defined (lowest, low, medium, high, and maximum) and Custom to set the scan intensity

Performance Settings

☒ Pre-defined ☐ Custom

Scan Intensity

Low

of HTTP Threads: 2

Password bruteforcing – enable this to find out how vulnerable your web applications are to password-cracking techniques

The following options are available under the **Search Criteria** section of an Option Profile:

Option Profile Creation

Turn help tips: On | Off Launch help

Step 3 of 5

1 Profile Details

2 Scan Parameters

3 Search Criteria

4 Comments

5 Review And Confirm

Please define what you want to scan for

Detection Scope

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection*

Core

☐ Include additional XSS payloads (may significantly increase scan time)

View list of Core QIDs.

Note: All Information Gathered QIDs will be included in scan detection scope when Core scope will be selected.

Sensitive Content

☐ Credit Card Numbers
☐ Social Security Numbers (US)
☐ Custom Contents

Cancel

Previous

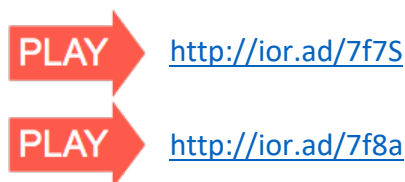
Continue

Detection Scope – This determines the vulnerabilities that will be checked during the scan:

- Core – Default for new WAS Option Profiles. Core scope includes vulnerabilities that Qualys considers most common in today's web applications. It does not include all the vulnerabilities that WAS can detect.
- Categories - Specific vulnerabilities defined in the categories. Select a category to check for associated vulnerabilities in the scan.
- Custom Search Lists - Specific vulnerabilities defined in Search Lists. This provides the most granular control over detection scope. You can select search lists to include and Search Lists to exclude.
- XSS Power Mode - Comprehensive tests for cross-site scripting vulnerabilities. The XSS Power Mode detection scope performs tests using the standard XSS payloads, which detect the most common instances of XSS, but also with additional payloads that can identify XSS in certain, less-common situations.
- Everything – All the vulnerabilities that WAS can detect.

Sensitive Content - Check for sensitive content in the web application pages it crawls based on known patterns (such as credit card numbers, social security numbers) or based on custom patterns you enter.

Qualys Browser Recorder Crawl Script



Web applications often contain pages that require input from a knowledgeable application user, like the “Shopping Basket” page found in the BodgeIT Store.

The QBR allows you to record your input decisions (e.g., keystrokes and mouse clicks) while you navigate the pages of any Web application. The script that is generated by QBR can then be replayed during your WAS scans, to perform your navigation steps and input decisions.

Detailed usage instructions for QBR can be found here - <https://www.qualys.com/docs/qualys-browser-recorder-user-guide.pdf>

The crawl script can be uploaded to an application. This will cause the application to be crawled using the script.

Web Application Edit: My First App Turn help tips: On | Off Launch help

Edit Mode

- Asset Details
- Application Details
- Scan Settings
- Crawl Settings**
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring

Add Selenium scripts to help us access different parts of your web application

Selenium scripts (*) REQUIRED FIELDS

Import the Selenium scripts to be used for scanning this web application. Each script runs one time when its trigger is first encountered by our crawler. Use Qualys Browser Recorder to create a Selenium script. Want to learn more? Watch this [video](#) or visit the Qualys Browser Recorder (QBR) [chrome extension](#).

+ Add Script

Script Name	Download	View	Change	Remove
crawlscript				Remove

Specify URL or [regular expression](#) to trigger this script*

☐ Use Regex

Specify a [regular expression](#) to verify that the script completed successfully.

☐ Run only after form authentication was successful

When the scan is complete, look for QID 150100 to check for Selenium Diagnostics:

Information Gathered Details

150100 Selenium Diagnostics

Finding #	3464704	Web Application	My First App
Unique #	022f57dc-ce14-401a-ab45-775ae3ae7d07		
Group	Scan Diagnostics	First Time Detected	14 Oct 2020 10:58AM GMT+0100
CWE	—	Last Time Detected	14 Oct 2020 10:58AM GMT+0100
OWASP	—	Last Time Tested	14 Oct 2020 10:58AM GMT+0100
WASC	—	Times Detected	1 View History...

Details

Results

Log for Selenium script: crawlscrip
Executing: |open | http://54.173.177.208:8080/bodgeit/home.jsp | |
Executing: |click | link=Widgets | |
Executing: |click | link=Weird Widget | |
Executing: |click | id=submit | |
Executing: |click | id=update | |

The authentication script can be used to create an authentication record.

Web Application Authentication Record Edit: QBR Authentication Record Turn help tips: On | Off Launch help

Edit Mode

Basic Information >

Form Record >

Server Records >

Comments >

Action Log >

Set credentials used to authenticate against web application.

Record Information (*) REQUIRED FIELDS

Enter the details for the login form. One of the easiest ways to find the form values is to view the source code and search for "<form" (without the quotes). Most browsers allow you to view the source either through the "View" menu or by right-clicking on the page.

There may be several forms on the page. Be sure to copy details from the form that contains the login fields.

Type*
Selenium script

Selenium (Automated Authentication)

Import the Selenium script to be used for authentication to web applications using this authentication record. Use Qualys Browser Recorder to create a Selenium script. Want to learn more? Watch this [video](#) or visit the Qualys Browser Recorder (QBR) [chrome extension](#).

Script: **authscript** [Download](#) [View](#) [Change](#)

Specify a [regular expression](#) to verify that the authentication completed successfully.

Validation Regular Expression*
successfully

WAS Reporting

 <http://ior.ad/7fmi>

 <http://ior.ad/7ff3>

Currently, the Qualys Web Application Scanning service offers 4 types of reports: Web Application Report, Scorecard Report, Scan Report, and a Catalog Report.

Web Application Report – Reports on aggregated findings from all scans.

Scan Report – Reports on findings from specific scans.

Scorecard Report – Provides an overall scorecard with high-level numbers and graphs.

Catalog Report – Provides a catalog of web services processed from completed maps, vulnerability scans and WAS scans.

Vulnerability status – Web application reports show the status of vulnerabilities, it may be one of the following:

- New – vulnerabilities discovered for the first time in the latest scan
- Active – open vulnerabilities that have discovered more than once
- Fixed – vulnerabilities that have not been found in the latest scan
- Re-opened – vulnerabilities marked as fixed but detected again on the latest scan
- Ignored – vulnerabilities marked as ignored

Vulnerability Details ✕

150012 Blind SQL Injection

[Install](#) [Patch](#) [Ignore](#) [Retest](#) **New**

URL: <http://54.173.177.208:8080/bodgeit/login.jsp>

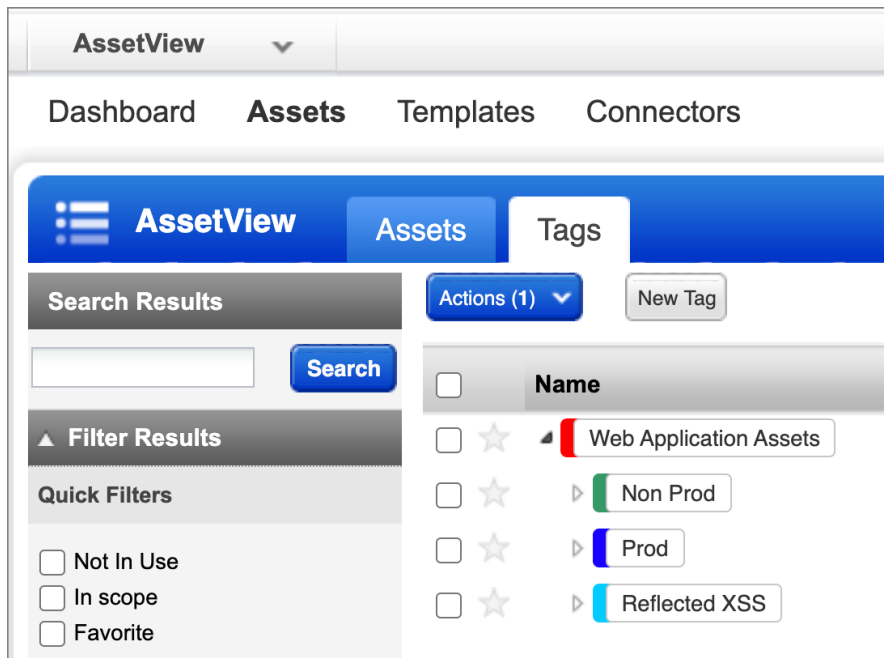
Finding #	8912890	Web Application	My First App
Unique #	ced8be32-a497-4d31-9570-ab9d235effb7	Authentication	Not Used
Patch #	–		
Group	SQL Injection	First Time Detected	14 Oct 2020 10:58AM GMT+0100
CWE	CWE-89	Last Time Detected	14 Oct 2020 10:58AM GMT+0100
OWASP	A1 Injection	Last Time Tested	14 Oct 2020 10:58AM GMT+0100
WASC	WASC-19 SQL INJECTION	Times Detected	1 View History...
CVSS Base	9.3	External References	–
CVSS Temporal	6.8		

Vulnerability Status

Tagging

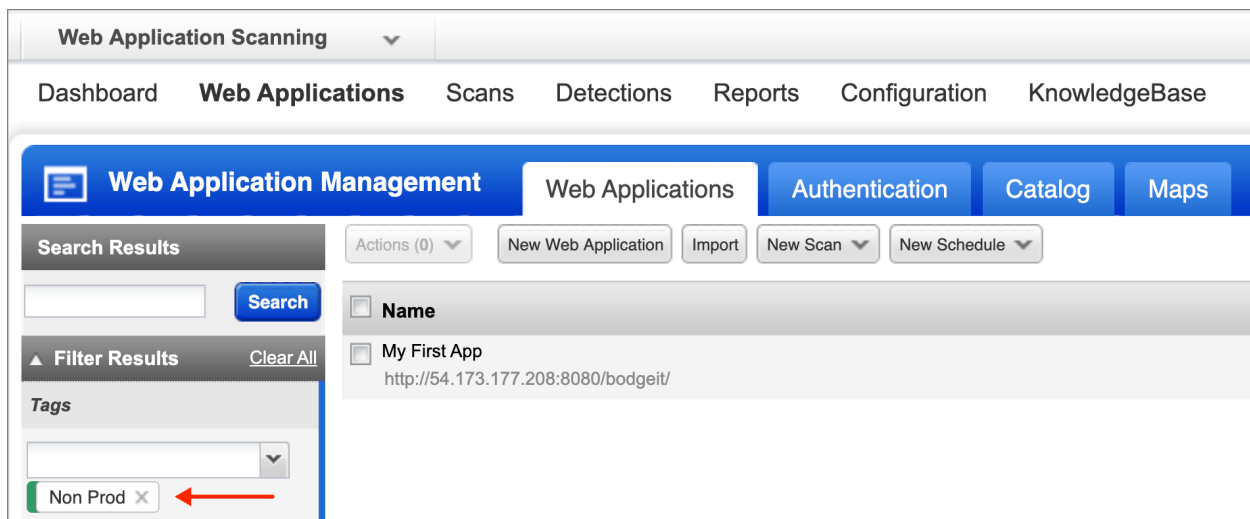


Tags are labels that can be applied to web applications. Tags can be used for filtering, scanning, and reporting purposes.



Tags are created from the AssetView application.

Use Tags for Filtering:



Use Tags for Scanning:

Launch New WAS Vulnerability Scan Turn help tips: On | Off Launch help

Step 1 of 3

- 1 Scan Details ✓
- 2 Scan Settings
- 3 Review And Confirm

Name your scan and configure target to be assessed

(*) REQUIRED

Scan Name*

Scan Target

Tell us the web applications you want to scan for security risks.

☐ Names ☒ Tags ←

Include web applications that have **All** of the tags below. [Select](#) | [Create](#) | [Remove All](#)

Prod x

Non Prod x ←

Use Tags for Reporting:

Report Creation Turn help tips: On | Off Launch help

Step 2 of 2

- 1 Details ✓
- 2 Target

Select target of your report

(*) REQUIRED

Select tags and/or web applications to report on.

Select Tags

Include web applications that have **All** of the tags below. [Select](#) | [Create](#) | [Remove All](#)

Web Application A... x ←

Exclude web applications that have **All** of the tags below. [Select](#) | [Create](#) | [Remove All](#)

Non Prod x ←

User Management



Users can be created from the Vulnerability Management (VM) or the Administration module. Once the user is created and activated, they will need to be given a scope and set of permissions from the interface.

Role Creation

To assign permissions to a user, first create a role from the Administration module. The role allows you to define the applications the user will have access to, how the user is allowed to access (UI or API), and permissions the user will have on the allowed applications.

Role Creation Turn help tips: On | Off

Step 2 of 3

- 1 Role Details ✓
- 2 **Permissions** ✓
- 3 Review And Confirm

Edit permissions for this role

Select how users would access this application

☒ **UI Access** ☐ **API Access**

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules

Role Permissions by Modules (63) [Remove All](#)

WAS Web Application Scanning [Remove](#)

- ▶ **WAS Asset Permissions (8 of 8)**
- ▶ **Scanner Appliance Permissions (1 of 1)**
- ▼ **WAS Scan Permissions (2 of 3)**
 - ☒ **Launch WAS Scan**
 - ☒ **Cancel WAS Scan**
 - ☐ **Delete WAS Scan**

[Cancel](#) [Previous](#) [Continue](#)

By assigning the role to the user's profile, you can define the permissions available to the user. The scope of the user can be limited by attaching tags to the user's profile.



Edit Mode

User Details >

Profile Settings >

Roles And Scopes >

Action Log >

Account Activity >

Edit role(s) and scope

☐ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role

Search unassigned roles

Assigned roles

Remove all ▲

WAS SCANNER

Remove

Unassigned roles

Add all ▲

AUDITOR

Add

CA MANAGER

Add

CLOUDVIEW User

Add

CONTACT

Add

CS User

Add

Edit Scope

☐ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope

Select | Create | Remove All

Prod X

Cancel

Save

Burp Integration



Qualys offers integration with Burp. Burp is an attack proxy used for automated and manual penetration testing. This can be used in tandem with Qualys for sensitive applications that need thorough testing.

With this integration, Burp Suite Professional (BSP) results can be uploaded to Qualys. This allows Qualys to act as a centralized storage location for scan results from Burp, to go along with the results already obtained by the Qualys WAS service.

Burp Report Import Turn help tips: On | Off Launch help

Select XML Burp report to import

Report Date
15 May 2013

Burp Version
1.5.08

Issues
33

Size
420.6 KB

(*) REQUIRED FIELDS

Import Settings

Select the web application associated with this report. Burp report contents show that issues have been detected for host **54.243.54.81**.

Web Application

My First App

[View](#)

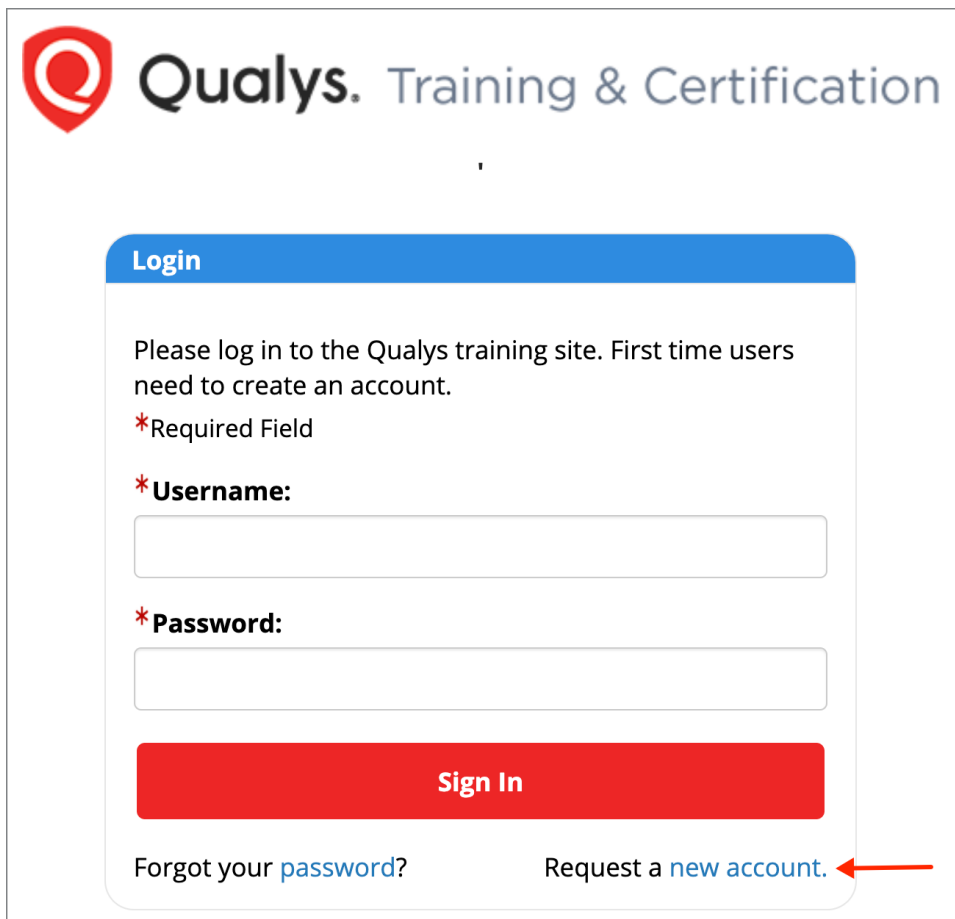
☐ **Purge web application Burp issues before import.**
If option is checked, all previous issues for the web application will be removed before import report issues.
Recommended to avoid duplicate findings when you are importing from multiple Burp instances.

☒ **Close existing issues not reported anymore.**
If option is checked, existing issues not reported in this report will be marked as Fixed.

When importing BURP results into WAS, the BURP results must be associated with a specific Web Application.

Qualys WAS Certification Exam

Participants in the Qualys Web Application Scanning and API Security training course have the option to take the Web Application Security Certification Exam. This exam is provided through our Learning Management System (LMS) at qualys.com/learning – candidates will need an account on this system to take the exam.



The image shows a screenshot of the Qualys Training & Certification login page. At the top left is the Qualys logo, a red shield with a white 'Q'. To its right is the text 'Qualys. Training & Certification'. Below this is a blue header bar with the word 'Login' in white. The main content area has a light gray background. It contains the text 'Please log in to the Qualys training site. First time users need to create an account.' followed by a red asterisk and the text '*Required Field'. Below this are two red asterisks followed by the labels '*Username:' and '*Password:'. Each label is followed by a white input field with a light gray border. Below the input fields is a large red button with the text 'Sign In' in white. At the bottom of the form, there are two links: 'Forgot your password?' and 'Request a new account.'. A red arrow points to the 'Request a new account.' link.

Qualys. Training & Certification

Login

Please log in to the Qualys training site. First time users need to create an account.

*Required Field

*Username:

*Password:

Sign In

Forgot your [password?](#) Request a [new account.](#)

If you would like to take the exam, but do not already have a “learner” account, click the “Request a new account” link, from the LMS at <http://qualys.com/learning>.

Once you have created a “learner” account (and for those who already have an account), click the following link to access the “Qualys Web App and API Security – QSC 2021” course page:

<https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?id=22511237829>

Course Catalog: Class Details
Course: Web Application Scanning and API Security - QSC 2021 Close Record

To see how a class below fits into your schedule, click View My Class Schedule.

CLASS DETAILS: WAS - VEGAS - QSC 2021
Course Name: Web Application Scanning and API Security - QSC 2021
Class Name: WAS - Vegas - QSC 2021
Class Code: 2250729076520210917131505
Contact Name: Shyam Raj
Private Class: Yes
Maximum Class Capacity: 150
Class Cost: \$0.00

Session Name	Location	Classroom	Address 1	Address 2	City	State	Postal Code	Times	Instructor(s)
Session 1	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom B	3600 Las Vegas Blvd. South.	N/A	Las Vegas	N/A	89109	Monday, November 15, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Shyam Raj

View My Class Schedule Enroll

Click here to Enroll

From the “Qualys Web App and API Security – QSC 2021” course page, click the “**Enroll**” button (lower-right corner).

After successfully completing the course enrollment, click the “Launch” button, for the Qualys Web Application Scanning Exam.

Class Name	Date	Location	Classroom	Instructor(s)
WAS - Vegas - QSC 2021	Monday, November 15, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom B	Shyam Raj

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Last Accessed	Time Taken	Attempts	Action
Qualys Web Application Scanning Exam	Actual Test	N/A	Not Attempted	N/A	N/A	N/A	Launch

Each candidate is provided five attempts to pass the exam.

Web Application Scanning and API Security - QSC 2021 Close Record

Progress: Completed **Status:** Enrolled **Required:** No **Duration:** 8 hours

Print Certificate

Activities

Class Sessions

Class Name	Date	Location	Classroom	Instructor(s)
WAS - Vegas - QSC 2021	Monday, November 15, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom B	Shyam Raj

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Last Accessed	Time Taken	Attempts	Action
Qualys Web Application Scanning Exam	Actual Test	97%	Passed	11/7/2021 9:33:29 AM	0h 11m	1	Launch

With a passing score of 75% (or greater), click the “Print Certificate” button to download and print your course exam certificate.

Training Survey

Please take a moment to take the survey about today's training - <https://forms.office.com/r/rsy0Aja6Xz>

Or scan the below link:

